

Aug 05, 2020

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information Associated with email address
RDCPRESIDENT87@GMAIL.COM/Google Account ID
429988766811

Case No. ~~20-CR-52~~ 20 MJ 165

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Please see Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

Please see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 21, United States Code, Section 841(a)(1)	Distribution of controlled substances

The application is based on these facts:

Please see attached affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

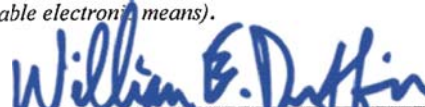


Applicant's signature

FBI SA Steve Whitecotton

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
email and telephone _____ (specify reliable electronic means).

Date: August 5, 2020City and state: Milwaukee, WI


Judge's signature

United States Magistrate Judge William E. Duffin

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, FBI SA Steve Whitecotton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (hereafter “Google”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Google Account that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been employed as such for approximately five years. I am currently assigned to a Criminal Enterprise squad in the FBI’s Milwaukee Field Office. My responsibilities include investigating violations of federal controlled substances laws and related violations, including federal firearms and money laundering offenses. I have had training regarding and participated in complex drug trafficking investigations.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

4. This affidavit is based on my training, experience, personal knowledge, and observations in this investigation; upon my discussions with other law enforcement officers and agents involved in this investigation; and, upon my review of official reports submitted in relation to this investigation.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that a violation of 21 U.S.C. § 841(a)(1) (distribution of a controlled substance) has been committed by Charles C. MCCOLLUM, aka “Cheese” or “Big Cheese” (B/M, 09/25/1987). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as further described in Attachment B.

JURISDICTION

7. The Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. In February of 2019, case agents initiated an investigation into a group of known and unknown drug traffickers operating in the Milwaukee area, known as the Buffum Meinecke Boys (“BMB”), including Ramone LOCKE, aka “Mone”, Amir LOCKE, aka “Big Mir”, Joey VAZQUEZ, aka “Joey”, Louis BATES, aka “Little Louis”, Michael SMITH, aka “M&M”, Garrell

HUGHES, aka “Rello”, Jesus PUENTES, aka “JP”, Coury AGEE, aka “Lil C”, Lamar JOHNSON, aka “Fresh”, Luis Lorenzo, aka “Pito”, and others. As part of the investigation, case agents have interviewed several confidential sources, conducted physical and electronic surveillance, utilized pen registers, reviewed historical phone toll records, subpoenaed and reviewed records, and conducted controlled purchases of cocaine, crack cocaine, and heroin. As a result of the intelligence provided by the confidential sources and the controlled purchases, along with information obtained from other law enforcement techniques, case agents have identified various members of the BMB and identified several sources of supply.

9. A particular confidential source hereinafter designated as CS #3 stated to law enforcement that MCCOLLUM has been known to supply heroin to various members of the BMB, primarily operating in the area of 19th St. and W. Atkinson Ave. in Milwaukee. CS #3 estimated that MCCOLLUM is responsible for kilogram-level quantities of heroin, trafficking through both the BMB and others.

10. Throughout the course of the investigation of the BMB, case agents have made several controlled buys of narcotics from members of the BMB. Based on my training and experience, I know a “controlled buy” is a law enforcement operation in which an informant purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded purchase money. When an informant is used, s/he is searched for contraband, weapons, and money before the operation. The informant is also wired with a concealed body recorder and/or a monitoring device. When the transaction is completed, the informant meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The informant is again searched for contraband, weapons, and money and then interviewed by the case agents about the drug

transaction. A sample of the suspected drugs is then field tested by the case agents for the presence of controlled substances and placed in inventory pursuant to normal inventory procedures. All of the calls to the target by the informants are consensually recorded calls under the direction and control of case agents and made in the presence of case agents. Additionally, case agents observe the informants dial the target's number on each occasion and the contact is verified through telephone records.

11. On February 6, 2020, case agents met with CS #3 to conduct a controlled purchase of heroin from MCCOLLUM. CS #3 first conducted a consensually recorded telephone call to MCCOLLUM via (414) 793-2769, which was verified by case agents. CS #3 placed an order of heroin from MCCOLLUM. MCCOLLUM then directed CS #3 to the area of N. 18th St. and W. Hampton Avenue in Milwaukee, Wisconsin. CS #3 travelled to the designated area and ultimately made contact with MCCOLLUM near N. 18th St. and N. Parkway Ave. Law enforcement observed CS #3 enter a black sedan, remain in the black sedan for a short time, return to his vehicle, and depart for a predetermined meeting location. At a subsequent meeting with law enforcement, CS #3 gave law enforcement the suspected heroin and told law enforcement that MCCOLLUM had provided him with the same in exchange for the controlled buy money. Case agents later subjected a sample of the suspected heroin recovered by CS #3 to testing via the Nark II 11/33, which showed a positive result for opiates, with a weight of 103.45 grams. Additionally, after the transaction, surveillance observed the black sedan park on the street in front of 4661 N 19th St., Milwaukee, WI. Surveillance then observed a black male matching MCCOLLUM's physical description exit the vehicle and walk towards the residence at 4661 N 19th St.

12. For several reasons, case agents believe CS #3 to be credible and reliable. First, CS #3 has been providing continuous information since September of 2019. Second, the information

provided by CS #3 is consistent with evidence obtained elsewhere in this investigation where CS #3 was not utilized, and substantial portions of CS #3's information have been corroborated through independent investigation, including surveillance and information from other sources. CS #3 has previously misstated one fact to law enforcement, but CS #3 corrected that error within the hour. CS #3 is cooperating for monetary compensation and has prior felony convictions for armed robbery, heroin trafficking and marijuana trafficking. CS #3 is currently on state supervised release.

13. On February 21, 2020, an arrest warrant for MCCOLLUM was issued in the Eastern District of Wisconsin, for the violation of Title 21, United States Code, Section 841(a)(1), (b)(1)(B) described above (distribution of a controlled substance; more specifically, over 100 grams of heroin). Subsequently, on February 25, 2020, MCCOLLUM was arrested at 3018 North 41st Street, Milwaukee, Wisconsin, pursuant to the aforementioned arrest warrant.

14. On March 3, 2020, MCCOLLUM was indicted in the Eastern District of Wisconsin for knowingly and intentionally distributing 100 grams or more of a mixture and substance containing heroin, a Schedule I controlled substance, in violation of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(B)(i), and Title 18, United States Code, Section 2. *See United States v. McCollum*, 20-cr-52 (E.D. Wis.).

15. At the time the foregoing indictment was returned, MCCOLLUM was on federal supervision, after pleading guilty to conspiracy to distribute heroin in Case No. 14-CR-61 (E.D. Wis.). As part of his supervised release in that matter, MCCOLLUM previously told his probation officer in that matter that his phone number is (262) 412-7331.

16. Law enforcement served a subpoena on Google seeking, *inter alia*, the names of email addresses associated with the phone number MCCOLLUM provided his probation officer:

(262) 412-7331. In response to that same subpoena, Google identified RDCPRESIDENT87@GMAIL.COM as an email address associated with telephone number (262) 412-7331. Additionally, Google explained that the email address RDCPRESIDENT87@GMAIL.COM was associated with a Google Account ID 429988766811, and identified the subscriber of the aforementioned email account/Google Account as MCCOLLUM. The email account/Google Account at issue was created on May 24, 2019. As more fully explained below, records associated with that same email account/Google Account are likely to contain evidence probative of MCCOLLUM's drug trafficking activities.

BACKGROUND CONCERNING GOOGLE

17. Google is an American multinational technology company that offers to the public, through its Google Accounts, a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome and a free search engine called Google Search.

18. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device.

19. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the login username for access to the Google Account. Enterprises may also establish Google Accounts which can be accessed using an email address at the enterprise's domain (e.g. employee[@]company.com).

20. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

21. **GMAIL:** Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

22. **CONTACTS:** Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their mobile phone or device address book so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

23. **CALENDAR:** Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple

calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device address book so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

24. **GOOGLE TASKS and GOOGLE KEEP:** Google also provides online to-do lists and notepads for Google Accounts. Google Tasks allows users to assign themselves tasks to be completed at scheduled times and marked complete when done. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.

25. **WEB-BASED CHATS and MOBILE MESSAGING:** Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.

26. **GOOGLE DRIVE:** Google Drive is a cloud storage service automatically created for each Google Account. Users can store documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents,

until they hit the storage limit. Users can also set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

27. **GOOGLE PHOTOS:** Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

28. **GOOGLE MAPS and GOOGLE TRIPS:** Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

29. **GOOGLE PLAY:** Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

30. **GOOGLE VOICE:** Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

31. **GOOGLE CHROME:** Google offers a free web browser service called Google Chrome, which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

32. **YOUTUBE:** Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

33. **INTEGRATION OF GOOGLE SERVICES:** Google integrates these various services to make it easier for Google Accounts to access the full Google suite of services. Users

accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

34. **SUBSCRIBER RECORDS:** When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

35. **ACCESS RECORDS:** Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use

an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

36. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

37. **BROWSING, SEARCH, and APPLICATION USE HISTORY:** Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely, unless the user deletes them.

38. **LOCATION HISTORY:** Google collects and retains data about the location at which Google Account services are accessed from any mobile device regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the

Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely, unless the user deletes them.

39. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings, those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

40. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. I also know, from my training and experience, that individuals who activate a Google Account for the purposes of only using a particular Google service (commonly email) will frequently generate records related to other services available with a Google Account, even inadvertently. This evidence may establish the “who, what, where, when, why, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

41. For example, the stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. Based on my training and

experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

42. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). This sort of location data—in addition to the Location History information described above—is especially pertinent where, as here, there has been criminal activity at a specific location, and law enforcement must work to confirm the identity of individuals at that specific location.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the Google

Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). In my training and experience, I know that drug traffickers typically use a wide variety of electronic media, including emails, to communicate with customers, associates, and sources-of-supply, and review of such communications can yield valuable evidence of this sort.

44. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

45. Therefore, Google's servers are likely to contain stored electronic communications and information concerning MCCOLLUM and his use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation, including information that can be used to identify the account's user or users, their location(s) and activities at certain times relevant to the offenses at issue, the identities of their accomplices and co-conspirators, communications with those accomplices and co-conspirators, and actions taken and research performed relating to the criminal offenses at issue.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

46. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information

(including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information which is associated with email address RDCPRESIDENT87@GMAIL.COM/Google Account ID 429988766811, which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the “Provider”):

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A for the time period of May 24, 2019 through February 25, 2020:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;
- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity, including: search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;
- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service

(such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- **MEDIA AND APPLICATIONS:** All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files; details of the associated device and Android ID for each application, medium, or file; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Google Voice

- **GOOGLE VOICE:** All Google Voice records associated with the account, including: associated telephone numbers, including forwarding numbers; connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history;
- **GOOGLE VOICE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on Google Voice, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery

numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;
- languages of input and output; and all associated logs, including access logs, IP addresses, timestamps, location data, and change history;

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of the violation of federal law, including, inter alia, the unlawful distribution of narcotics in violation of Title 21, United States Code, Section 841(a)(1), for the account listed in Attachment A, information pertaining to the following matters:

- a) Information that constitutes evidence concerning the unlawful distribution of narcotics;
- b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- e) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

- f) The identity of the person who created or used the user ID, including records that help reveal the whereabouts of such person; and
- g) The identity of the person(s) who communicated with the user ID about matters relating to the unlawful distribution of narcotics, including reports that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.